Maximization of Transit Security Through Effective Use of Procedures

JOHN N. BALOG, ANNE N. SCHWARZ, WILLIAM T. HATHAWAY, AND LARRINE WATSON

FTA's safety and security program goal is to achieve the highest practical level of safety in all modes of transit. To protect passengers, employees, revenue, and property, all transit systems are encouraged to identify, evaluate, and adopt security procedures that are most efficient and effective in local practice. Both proactive and response procedures should be included along with methodologies for reviewing their effectiveness. The materials in the *Transit Security Procedures Guide*, which was produced by Ketron while under contract to the Volpe National Transportation Systems Center, are summarized. The guide was designed to make systems aware of the procedures used across the country by transit security specialists. The summary includes information on applying the system's approach to transit security planning and implementation, proactive materials for the prevention of security incidents, procedures for immediate and follow-up response to security incidents, and a specific evaluation methodology for security problems including crimes against passengers, crimes against the transit system, crimes against the public (hostages, hijacking, bomb threats), and general issues. The methodology includes information on the most important attributes of each security problem: severity, frequency, type, areas of effect, when, locations, contributing factors, solutions and approaches, personnel costs, facility and equipment cost, effectiveness, and application.

The security of a transit system is an integral part of the service that it provides to its riders. Passengers perceive it as the responsibility of the system to ensure that they are safe. If passengers are not safe, the system is failing its responsibility. Passenger perceptions affect system ridership and revenue. The system is also responsible for the security of its own personnel, facilities, and equipment.

This paper summarizes a product developed by Ketron for the Volpe National Transportation Systems Center and FTA entitled *Transit Security Procedures Guide*. It represents a compilation of available materials into a single, usable guide that incorporates the necessary information for planning and improving transit security. The information is designed to be used by transit planners, security personnel, and managers in the development of their plans, procedures, and capital programs. A central tenet is to encourage systems to take a proactive systemwide approach to security.

The systems approach includes examining all aspects of the system and evaluating potential security risks. It involves planning for security before the incident rather than reacting. This approach has several advantages. First, it allows an examination of how all aspects of the system interact to affect security, including personnel, procedures, equipment, communication, and passengers. A second advantage is that security risks and the measures needed to mitigate them can be identified before an actual security problem develops. Preventative measures can be applied and the dangers, problems, and resulting costs can be avoided. The third advantage is that security measures can be implemented in a cost-effective manner if they are incorporated in the planning stages of facilities, personnel training, and equipment purchases.

Systems need to reduce risks to passengers, personnel, and equipment. Planning and anticipating security risks can limit the number of incidents and reduce their consequences. Reacting to a security breach is costly. For example, if fares are stolen, revenue is lost. Even if the perpetrator is found, recovery of the lost fares may not be possible. Without the installation of effective countermeasures, such as observation cameras, alarms, and security procedures, there may not be a means for locating the perpetrator at all.

A breach in security can also have an effect on the morale of employees, who will feel more at risk. In addition, there can be a negative affect on the perceptions of passengers, who will feel that they are not adequately protected. These costs can be reduced if countermeasures are in place, such as observation of the incident to aid in identifying the perpetrator, procedures for raising an alarm for when the perpetrator leaves the vehicle or the facility, storage of some of the fares in inaccessible safes, and existing procedures for apprehending the offender.

Security planning involves identifying possible areas of security threats, assessing the magnitude of the threats and the vulnerabilities of the system to them, planning for the resolution of the threat, and following up the security breach with an evaluation of procedures, plans, and policies to address any errors and implement necessary changes.

Each system's security program must address its particular needs and the particular threats that can be identified during security planning. Each system is different and will be able to identify particular areas of risk. Each system will also have differing levels of resources to address those risks. The procedures discussed here provide the information necessary to rank system needs and to allocate resources effectively.

Preventing security incidents is a major topic. This paper describes methods for developing preventative procedures and discusses staffing, equipment, features, and hardware that can address the security risks that systems face. A systems approach is used to examine preventative measures in all aspects of the system, from the point of view of the passenger, transit personnel, and the risks to the equipment and facilities. All security aspects of the system are interrelated. Staffing of facilities has an effect on overall security, as does the design of facilities. Choices of equipment and security systems are affected by the types of facilities and the

J. N. Balog and A. N. Schwarz, Ketron Division of the Bionetics Corporation, 350 Technology Drive, Malvern, Pa. 19355. W. T. Hathaway and Larrine Watson, Volpe National Transportation Systems Center, 55 Broadway, Kendall Square, Cambridge, Mass. 02142.

level of staffing. At the same time, equipment choices can affect staffing levels and the types of design features incorporated into facilities. Information necessary to make informed choices and to be certain that the choices made are addressing the particular security needs of the system are presented.

The second major area discusses security responses and offers information on the actions that systems should take if there is an incident. Actions include immediate response, communication, follow-up, and reporting. Each needs to be defined and described in the passenger, vehicle, and facility system security program plan. Transit personnel need to know what response is expected of them when a security incident occurs, what to do to help prevent an incident from escalating, and how to minimize the effects of the incident on passengers and facilities. Follow-up and reporting are also important for evaluating the causes of security incidents and improving methods for preventing them. Effective follow-up and reporting allow the system to learn from incidents and to prevent them in the future. Systems can use this information to develop their necessary response procedures.

The third major section addresses special security problems. It considers a variety of problems experienced by transit, including crimes, misdemeanors, and annoyances, through the use of an evaluation format. Security problems can be difficult to solve. They often require ongoing procedures and can require urgent attention. The format includes the types of procedures that can be successful in different types of systems, special security problems from the perspective of potential solutions, and solutions as to their cost and effectiveness and the type of application necessary for a successful approach.

This paper is a summary of the full *Transit Security Procedures Guide*. Consequently, the specificity of the information presented is lower than in the full document. However, significant information is conveyed. Positive results can be achieved by following the suggested program; the number of security incidents should be able to be reduced and the consequences of the actual realized security incidents should be minimized.

PREVENTION OF SECURITY INCIDENTS

Every system should have a security plan and security director. The number of system employees, whose primary function is security, will vary depending on the size of the system and the approach to security staffing. However, security is the responsibility of every employee. This section discusses the system's concerns and alternatives in security with regard to staffing. Details on the considerations necessary for a complete staff of security officers are provided, as well as discussion of the roles of personnel whose primary function is not usually security but who do play a vital role: operators, clerks, and other staff.

The section concludes with a discussion of coordination with local police departments—an extremely important element of all security programs, regardless of the size or makeup of the system. The materials in this section will not dictate what type or level of staffing is best for all systems. Presented here are the alternatives. The security department referred to throughout may be a staff of several thousand transit police and support staff, or a single security, safety, and training officer, depending on the needs of the system.

Persons responsible for patrolling buses, guarding facilities, and responding to incidents may come from a variety of sources, including

- Local police (including state police in rural areas),
- Local police with special transit units,
- Contract police and security services,
- Transit police, or
- Some combination of the preceding.

Each of these approaches has merit.

All systems rely on local police forces to some extent. Smaller systems may rely exclusively on local forces. This arrangement is entirely appropriate if the security needs of the system are being met. Reliance on local police may be the best arrangement if the jurisdiction of the local force includes all or most of the transit service area.

If the system relies on local police, it would call the police to respond to any serious violation. Minor security incidents would be handled by in-house security staff or an operational supervisor. The security department would be primarily administrative and operational. The system may employ staff to identify problem spots to keep the local authorities informed. Although the system might additionally employ patrol guards, the rest of the in-house security staff would commonly be supervisors, station attendants, and spotters. The tasks of in-house security staff might also include locking up, inspecting the facility, reporting incidents, and providing a human presence.

Some systems rely on a special division of the local police department to provide policing services. The system can work out arrangements with local authorities for qualifications required for the transit unit staff. Typically the special transit team is a respectable if not elite assignment. The system may provide a great deal of orientation to these officers and involve them in operator training to help officers understand how transit operations occur. Special transit units often do not provide services that satisfy all the security needs of the transit system. Other security staff may watch facilities at night, guard revenue transfers, and perform administrative functions.

This type of arrangement represents a compromise between a separate transit police force and complete reliance on a police force that provides general services to a large area. The special unit has complete familiarity with the system and ongoing security problems but can draw on the same support resources as the local forces. Complications of transit security coordination with local forces are avoided because the officers are working through local forces. Additional manpower can be easily brought in as needed, drawing from the rest of the local force.

To establish a greater degree of control and to avoid the difficulties of administering a full staff, some systems contract for security services. By hiring the services of a number of officers, from a single firm or police force, the system can detail through the contract the exact requirements of the services. In some cases the system and security company together establish a pool of individuals from which to draw.

The security forces must report to at least one person in the system, although it is possible to contract out for both the staff and management of the security force. An individual or office within the system, however, would have to monitor the performance of the contractor and provide guidance and expectations.

Security officers contracted from private firms will not have full police powers. As security guards they may make citizen's arrests, detain individuals, and provide a uniformed presence and a rapid response, but they cannot make arrests and issue citations.

Transit systems with transit police forces require full police powers if the security staff is to be effective. Although security guards can deter less serious crime, police with full powers are needed to deter and respond to more violent crimes. In communities where transit crime is less often violent, police powers can do much to enhance the effectiveness of the force, but they may not be necessary.

An in-house force of transit police allows the system to rely less heavily on local forces but cannot eliminate the need for cooperation. Reporting functions need to be shared, and local forces must provide backup for the transit police. Often the local forces are more widely distributed geographically and in some cases will be able to respond faster. Furthermore, local police facilities are generally relied on for booking and holding functions.

Since it is always necessary to rely on and cooperate with the local police to some extent, it is extremely important that transit security staff command the respect of local forces. In the case of a transit police force, the local force may have to approve its creation before full police powers can be granted on a permanent basis. This is commonly achieved by setting high training and employment standards. It is often both convenient and useful to use the same standards as local police forces, even using the same training sites and local academies. Respect for the experience and capabilities of transit police is greatly enhanced by drawing staff from the local force, especially to serve as top officials. Salary rates are often based on the rates paid to local officers.

The use of a dedicated transit police force is especially appropriate when the system services many jurisdictions. The complexity of coordinating jurisdictional services can be greatly reduced through the use of a staff with full police powers that is responsible throughout the many locations that the system serves.

Selection of the appropriate approach is primarily a function of the size of the system, the number of political jurisdictions in the service area, and the need for the forces to have full police powers. For example, as the size of the transit system increases from small to very large, the progression is usually local police, local police transit units, contracted police services, to transit police. The upward progression also is associated with jurisdictions. With only one jurisdiction local police can often handle security. As the number of jurisdictions multiplies, transit police are most effective. If police powers are required, then the local police transit unit or transit police options are best.

Prevention of security incidents is dependent on the personnel available to provide policing services. In addition to the security functions of the operations staff, transit systems often use a variety of security personnel including sworn officers, security guards, patrol guards, spotters, locksmiths, inspectors, and supervisors. Selection of an in-house solution to security requires the acquisition of appropriate personnel. In addition, it often requires a significant capital investment in support equipment. The prevention of security incidents often requires equipment such as guns, chemical mace/pepper, handcuffs, batons, radios, bullet-resistant vests, badges, helmets, keys, disorder gear, uniforms, and vehicles. These items of equipment are effective in responding to security incidents and have a definite, positive, proactive value to the deterrence of security problems as a result of their visual presence.

Identifying and hiring security staff should be based on a specific set of minimum qualifications such as the following to ensure a highly capable force:

- Age preference (minimum/maximum),
- Height and weight (proportional),
- Interviews with security personnel or character investigators,
- Physical agility and dexterity,
- Physical fitness,
- Previous police or security experience of 1 to 5 years,
- Previous transit experience,
- Psychological character issues,
- Recommendations,
- Record checks, and
- General knowledge or aptitude.

Minimum qualifications should also be used if security manpower is contracted.

Additional costs result from the need to train personnel before putting them into service and then regularly thereafter to maintain required levels of readiness. Training should include

- Familiarization with existing and key procedures,
- Special weapons,
- Handling of the homeless,
- Public relations and assistance,
- Sensitivity training for victims, and
- Interjurisdictional coordination problems.

Security training should not be limited to security staff. All operations staff perform security-related functions, and their effective response and daily functions can be reinforced with refresher training and special courses. Ongoing training generally augments the morale of personnel, partly by providing a break from the regular routine and especially by extending the skills of individuals.

Coordination with local police departments is vital to the proper operation of any transit security program, especially emergency response. This coordination includes the sharing of information; agreement on roles, responsibility, and jurisdiction; setting up of communications; and cooperation during training, exercises, and operations.

Security can be an important factor in encouraging or discouraging rider use. Patrons' perceptions of security can be the major difference between transit users and nonusers. Transit security is generally perceived to be lower during off-peak hours because of the smaller numbers of people present and the effect of low light conditions. The perception of minimum transit security can keep off-peak ridership low during those hours. Improving off-peak security could do more to increase ridership at those times than operational measures such as increased frequency or destinations.

Individuals who have experienced a crime in the transit system, have witnessed a crime, or know someone who was a victim of a crime hold negative perceptions of transit security. However, most people's perceptions of security are unrelated to actual crime statistics. Passengers react to trash-strewn stations, evidence of vandalism, physical deterioration, graffiti, and other characteristics by perceiving a low level of passenger security.

In general, the public's perception of security depends on the visibility of protection efforts. Uniformed patrols are more effective than surveillance cameras. Surveillance cameras in plain view of passengers are more effective than hidden cameras. Surveillance cameras in conjunction with conspicuous booths where security personnel are watching monitors are more effective than security cameras alone. Good facility design features that ensure

complete visibility also improve the perception of security. People will not feel secure if they must enter a station from a deserted alley or walk through a tunnel with turns, around which someone could be hiding. A bridge over tracks is more visible than an underground tunnel. Stairs can be left open rather than walled. Open fences improve visibility in comparison with walls. Facility corridors need to have as few turns and barriers as possible. Mirrors so that people can see around corners are also important.

Facility maintenance is another factor in increasing perceived security. In addition to normal maintenance, it is important to remove all evidence of vandalism or graffiti quickly. Quick removal minimizes the number of people who will be aware of the lapse of security and demonstrates the responsibility and responsiveness of the system.

Whenever large numbers of passengers are near each other, their perception of security is maximized. It is therefore useful to integrate routes and modes of travel and decrease headways so that vehicles are frequently arriving and leaving any particular stop or station.

Procedures used by security forces can have an impact on rider perception of security. For example, if an individual has perpetrated a crime and is on a bus or train, the offender should not be approached until he or she is leaving the vehicle. Arresting an individual on a vehicle causes significant concerns to passengers. Similarly, a number of police at a facility or stop searching for an offender can suggest that the crime was violent and would cause negative perceptions.

Encourage anonymous passenger reporting of security incidents. Bystander apathy is typically related to the concern that the perpetrator will retaliate toward witnesses. The installation of equipment and procedures that allow passengers to report crimes in progress or to later report that they witnessed a crime will encourage them to contribute information that can lead to the incarceration of the offender.

The system also needs to encourage local residents associated with town-watch activities, tenant associations, and neighborhood meetings. Systems can be effective in showing cooperation or concern for their local neighborhoods by providing speakers and programs. It is also useful to establish relationships with youth groups and provide part-time or summer jobs to unemployed youths. It is not uncommon for many activities of graffiti and vandalism to be associated with youths. Bike patrols are also an effective means for quick reaction in response modes while still providing mobile visibility of the security force.

Often local celebrities and athletes have concerns for the community and can be approached and requested to be included in public service announcements, fairs, and other activities in which they can be viewed as role models. Using retired and specially equipped vehicles as mobile public relations sites can facilitate the distribution of security and other materials and make the local community aware of security devices such as lights, silent alarms, variable message sign boards, and two-way radio communication systems typically installed on vehicles.

Establish relationships with the local news media so that they know who to call when information is needed and a rapport can be established. The news media can sensationalize security incidents. They need to understand that balanced reporting is necessary to maintain the appropriate perception of security by passengers. Establishment of such a relationship facilitates the forward movement of publicity information that the system wants to convey.

Passenger relations training of operators is also important. Since operators must often take steps to control passengers, their calm, confident, helpful attitudes can contribute to a positive impression. When passengers are being rowdy and noisy, disobeying common rules, or committing vandalism during the ride, the operator has an obligation to control the passengers. Training can give operators the skills, confidence, and professionalism to handle troublesome passengers. Adequate control of passengers makes all passengers feel more secure.

RESPONDING TO SECURITY INCIDENTS

This section addresses ways in which a system can respond to criminal activities. Beginning with immediate response to an incident, it addresses security activities from the start of the incident through its review and follow-up to reporting. It also includes the special considerations of communications, interaction with law enforcement agencies, record-keeping and reporting, and on-going system refinement. This section addresses the reactive staff activities involved in system security.

Often a system employee will observe a crime taking place. The reactions of the initial observer can have a major impact on the outcome of the incident. There are three basic options to a person who comes upon a crime: do nothing, go for help, or try to intervene. The actions that they take should depend on how they are trained and what they observe. The objective is to stop the crime from proceeding without having it escalate.

Observers must base their reactions on what level of criminal activity is taking place. Types of crime can be divided into four categories:

- Nonviolent, nondestructive regulation violations such as eating or smoking in unauthorized areas or loitering;
- Nonviolent, destructive behavior such as fare avoidance, defacing system property, and pickpocketing;
- Violent, theft-related crimes such as robbery employing a weapon; and
- Violent, assault-related crimes such as fights.

Nonsecurity employees may be able to intervene in a nonviolent criminal activity and successfully stop it. On the other hand, they would be ill-advised to intervene in a violent crime situation because of the possibility of making matters worse. The ability of employees to be able to observe a crime, determine its level, and decide on what action should be taken is totally dependent on the training that they have been provided. Training that establishes procedures for reacting to each type of incident is needed. In addition, procedures should be practiced so that employee reactions are conditioned before an incident takes place.

Once information is received that a security incident has occurred, the operator or dispatcher is responsible for putting the response system in motion. There will be a wide range of possible actions depending on the type, magnitude, and location of the incident. Actions include

- Dispatching security personnel,
- Calling the police,
- Notifying supervisors and management,
- Notifying system dispatchers and route controllers,
- Establishing on-scene communication,

- Activating the general announcement system to relay messages,
- Calling for rescue or emergency support,
- Recalling off-duty personnel, and
- Informing the media.

Technology can be an effective force multiplier in attempts to cope with security problems. However, technology cannot substitute for motivated employees who take the security aspects of their job seriously and perform their duties professionally. Technology has the potential to act as a placebo, convincing some that the system is secure because there are cameras, alarms, communications, and sensors. Each of these items allows security personnel to monitor greater areas of the system than they could personally. But no matter how good the technology, the staff that monitors it must be alert, motivated, and trained to be effective.

Communications serve as the backbone for response to a serious crime. Primarily, they are as the command and control link to coordinate the response while the crime is in progress, but they can also help keep the situation from escalating, reduce public exposure to dangerous situations, and provide an accurate record of the activity surrounding the crime for later review and analysis.

The purpose of incident follow-up is threefold. First, it is to limit and repair any harm done to individuals and property. Follow-up response will initially focus on any people who were in the vicinity of the crime to alleviate their danger and to help in their recovery. It then focuses on limiting the danger to the system from any aftereffects of the crime. The second purpose of follow-up is to collect information and evidence from the incident for possible legal action and to evaluate the effectiveness of the security system. The third purpose is to return the system to normal operation. This will involve cleaning up the site, dispersing the crowd, reopening any areas that may have been closed, and handling the dissemination of information concerning the incident.

"Security would be so simple if it weren't for all of the paperwork": this is the attitude shared by many professionals. It is not surprising if the individual sees no benefit derived from the filling out of long, apparently useless forms. The reporting part of the security process needs to demonstrate its value in terms that directly affect the persons providing the information. Information requirements can differ depending on many of the same factors discussed earlier, including the size of the system, the environment in which it operates, the amount of crime that prevails, and the authority of the system itself. Reporting information includes tapes of telephone and radio communications involving the incident; legal materials, such as the records of incident investigations, arrest records, and custody records; quantitative data or numerical information, such as cost and time necessary to draw statistical conclusions; and qualitative information, which is often narrative and requires interpretation by the user to draw conclusions. All collected data must be securely stored, and the method most typically used is computers. Computers also provide the ability to serve as the basis for generating reports. A number of safety reporting software programs and data bases are in use in the United States that include some means of security data as well. Among them are two that have been developed and refined by FTA: AERS (Automated Emergency Response System) and SIRAS (Safety Information Reporting and Analysis System).

No matter how effectively a security system has been developed and applied, some flaws and problems can be identified only after specific incidents have occurred. The security system should be kept in top form. Steps to reach this level of readiness include reviewing the policies and procedures as a follow-up to an incident review team report. It may be that the policies and procedures used were inappropriate for the particular security incident. If so, new procedures will need to be developed. Such procedures should not be developed in a vacuum; they should be thought out very carefully while anticipating any ramifications to other security procedures. It is highly desirable to use training exercises to identify ways to defeat newly created procedures. Ultimately, once the bugs are worked out and the new procedures adopted, all employees should be retrained on the new procedures and they should be integrated into the program.

SPECIAL SECURITY PROBLEMS

General

The base document from which this summary was prepared includes many security problems that are fully discussed according to a classification scheme. The length of the paper does not allow for the discussion of the procedures, but the classification scheme is summarized. Each system may want to acquire a copy of the guide, study each of the various security problems, evaluate the solutions and techniques, and decide what they may want to do.

The basic format of this classification scheme is shown as in Figure 1. The name of the security problem or issue is shown in the upper left hand corner of the figure.

"Severity" is described as low, moderate, or high, depending on how much damage, how great an injury, and how much loss may occur based on a single incident.

"Frequency" indicates the relative likelihood of the incident occurring or how often the crime may occur, relative to other problems.

"Type" of security issue refers to whether the issue is considered a general security issue, a crime against passengers, a crime against the system, or a crime against the public.

"Locations" describes where the problem occurs the most, whether on the bus, rail, on-board any vehicle, in parking lots, at stops or shelters, in the adjacent community, at facility approaches and exits, in the vehicle front or rear, at entrance/exit areas, at fare collection areas, on the platform, in corridors, in offices and garages, in any location, or various other sites.

"Areas of effect" indicates what parts of the system may be affected most directly by the incident, including passengers, vehicles, equipment, facilities, staff, or all of these.

"When" describes what time of the day or what part of the passenger's trip the incident can occur. This descriptor varies significantly depending on the problem and might include whether the incident is likely to occur while patrons are waiting, boarding, on-board, exiting the system; during peak hour, off peak, business hours, rush hours, early a.m./evening, late night; while closed; at some special time; or at any time.

"Contributing factors" include those general conditions that cause a problem or make a security breach more likely. Examples include lighting, community, staff, presence of others, fare, approach of vehicle, observation, time of day, equipment strength, police presence, secrecy, response capabilities, history of an issue, human factors, equipment power, or various other factors.

"Solution areas" summarizes the *types* of approaches and areas affected by solutions. These areas vary but may include training,

SECURITY PROBLEM	Severity:	Frequency:	
Type:	Areas of Effects:		When:
Locations: Contributing Factors: Solution areas:			
SOLUTIONS/ APPROACHES:	Cost	Effectiveness	Duration
	Personnel / Facility/Equipment		

FIGURE 1 Summary table format.

equipment, facilities design, response, public relations, community relations, communications, observation, fares, advertising, coordination, cooperation, enforcement, special materials, and contingency planning, among others.

"Solutions/approaches" provides brief descriptions of possible solutions or approaches to handling the problems. Approaches are discussed in further detail within the text, but in this figure information regarding the costs, effectiveness, and period of application is summarized for comparison. Strictly speaking, all of the costs, effectiveness, and application periods are variable, but the relative merits and drawbacks are presented for quick consideration.

"Cost-personnel" describes the relative expense in staff time and salaries generally required to effectively implement and maintain the approach to security. These costs are presented as low, moderate, or high.

"Cost-facility/equipment" describes the relative costs of obtaining or maintaining capital including new equipment, devices, or facility improvements. They vary depending on how elaborate the specific materials. In general, however, they may be described as low, moderate, or high.

"Effectiveness" notes how effective this solution or approach should be, how effective other systems have found this to be, and how likely the approach is to work alone. The real effectiveness of a program will be determined by how well it is implemented and the specific problem that it is designed to address; however, the relative effectiveness of the approach compared to other approaches is described as slight, low, moderate, high, or very effective, or variable if there are an unusually high number of other factors that dictate the success of an approach.

"Application" describes how often the solution approach will have to be applied. Equipment-based solutions need to be installed only once, for example, but training approaches are required periodically. Efforts may be required once, for each case, periodically, or on an ongoing basis.

The classification methodology can be used to summarize all security problems. For purposes of discussion, security problems have been organized into several categories:

- General security issues,
- Crimes against passengers,
- Crimes against the transit system, and
- Crimes against the public (critical incidents).

General security issues include minor problems that must be handled on a daily basis by front-line transit personnel. These issues seldom require the intervention of police and are rarely reported. They also include security-related issues that may not result in harm to people or property during a single incident but have been ignored for some time. General security issues common to all transit systems include disorderly conduct, drunkenness, crowd control, drug law violations, minor sex offenses, solicitation, homelessness, and miscellaneous misdemeanors or nuisances, such as transit rule or local ordinance violations.

Crimes against passengers are serious but somewhat less frequent. They include theft, physical assault, and sexual assault. The nature of these crimes varies, and the approaches to addressing each particular problem can take many directions.

Crimes against the transit system are particularly common. They include fare evasion; fare theft; suicide attempts; vandalism; trespassing; theft, burglary, robbery; and security of personnel.

Crimes against the public are system crimes that are not limited to the security of the passengers or the transit system. Inherently, they are extremely critical incidents, such as hostage taking, hijacking, and bomb threats.

An example of the classification scheme as applied to the crimes against passengers problem of physical assault is offered.

Physical Assault

The potential for physical or sexual assault when using transit is a significant concern. Although the incidence of assault in transit is often comparable to or less than the incidence in the surrounding community, many people perceive that they are less secure while waiting for or riding on a transit vehicle. Personnel must create a secure environment and educate the riding public regarding positive steps to take to increase their security.

Types of Assaults

Assaults in transit systems can be categorized into two types. First, there are altercations that involve a single assailant and a single victim. The two individuals may know each other or they may be strangers. This type of assault is usually not planned and usually does not involve a weapon. It may result from the release

of aggression from the assailant, who is experiencing some frustrating circumstances (which in no way justifies the assault). This type of assault can occur in a number of locations, including a bus or train, a platform or stop, a station, a parking lot, or anywhere else in a transit system.

The general type of assault usually involves one or more victims confronted by a group of assailants. This type of assault is usually planned. It may not be designed for the actual victim but planned with the intent of assaulting someone. Often, the motive of this type of assault is robbery, but there are other common motives, including hate crimes (violence against certain ethnic, religious, or racial groups), crimes targeted at homeless individuals, and gang assaults of a random and seemingly inexplicable nature. These crimes take place in society at large, and transit systems are not immune.

Frequency of Physical Assaults

Assaults do not occur as often as less serious transit crimes, such as vandalism or fare evasion. The surrounding service area of the system usually determines the frequency of assaults: more often in high-crime urban areas, less often (or rarely) in small towns and rural areas. Assault victims are likely to report the incident to authorities, so the reported number of assaults in transit systems closely reflects the actual incidence.

Prevention of Physical Assaults

Systems must take measures that prevent assaults and reassure passengers that they can travel without fear of assault. The perception of security is just as important as the actual level of security. The system's actions should be very visible to both the potential criminal and the passengers. These actions include creating an environment that discourages assaults, employing visible transit security personnel, designing facilities to discourage assaults, installing closed-circuit television (CCTV), and installing alarms and call boxes.

Environment That Discourages Assaults

The highest priority should be placed on the safety and security of its passengers. As with all security problems, the most effective way to reduce the occurrence and severity of passenger assaults is to create an environment that discourages attempts. Preplanned assaults on passengers will more likely take place at times and locations where criminals believe their attack will go undetected and where escape from the scene of the incident is easy. Therefore, effective measures that a system should take involve the design and maintenance of the facility (stop or station), training of the operators and other personnel in the field, and specific security personnel and procedures.

Visible Transit Security Personnel

Visible uniformed security personnel are very effective in preventing assaults. The presence of other transit personnel, while less effective, may be more practical and require less additional expenditures. The fact that an assault will be immediately detected is the greatest deterrent to potential assailants.

Smaller transit systems may not have their own security personnel to patrol routes and stops. Instead, they rely on local police. In this case, the lead transit security officer should focus efforts in coordinating the system's resources and information with the local police department.

Facility Design To Discourage Assaults

Several facility design features are helpful in deterring assaults. Good lighting increases the likelihood that a passenger can see a potential assailant. Passengers will also feel more comfortable in a well-lit area. Areas that should be kept well-lit include station platforms, bus stops, and bus shelters.

Many rail systems have designated off-hours waiting areas in their stations. These are clearly marked portions of the station that are within sight of transit personnel. They are also part of the train platform or are close enough to the platform for easy access to arriving trains. Passengers are not required to wait at these off-hours areas, but they tend to do so, especially when encouraged through transit system promotions.

Closed-Circuit Television

An effective but higher-cost measure is the installation and use of a CCTV monitoring system. The presence of cameras at stations and platforms gives an impression to passengers and potential assailants that criminal activity will be detected. The use of CCTV enables staff to observe activities at a wide variety of locations and alert security personnel to report to a specific location when necessary.

Alarms and Call Boxes

Alarms and call boxes provide a means for passengers and transit personnel to call for assistance in the event of assault, threat, or some other emergency. Their locations must be planned for convenience of users. A transit system must also develop procedures for responding to the alarms or messages, including the inevitable false alarms. The effectiveness of alarms, call boxes, and CCTV is enhanced when used together.

Figure 2 shows the potential measures that transit systems can take to reduce assaults.

CLOSURE

In the adoption of procedures for preventing and responding to security incidents it is important to keep in mind several items.

- Fully identify, discuss, and determine how security can be proactive.
- Do not wait for security incidents to occur; anticipate them by reviewing literature and existing records and having discussions with other transit systems.
- For each and every security problem identified, formulate what solutions need to be put in place.

PHYSICAL ASSAULT	Severity: HIGH	Frequency: INFREQUENT
Type: AGAINST PASSENGERS	Areas of Effects: PASSENGERS	When: ANYTIME

Locations: Bus, Rail, Parking lot, Stop/shelter, Adjacent community, Platform, Corridors

Contributing Factors: Poor lighting, No police presence, No other staff presence, Awkward facility design

Solution areas: Enforcement, Equipment, Facilities design, Cooperation, Observation, Training

SOLUTIONS/ APPROACHES:	Cost		Effectiveness	Application
	Personnel	Facility/Equipment		
Coordination with local police force	LOW	LOW	VARIABLE	ONGOING
Visible transit security personnel	HIGH	LOW	HIGH	ONGOING
Presence of other transit personnel	LOW	LOW	MEDIUM	ONGOING
Good Lighting	LOW	MEDIUM	MEDIUM	ONGOING
Off hours waiting areas	LOW	LOW	HIGH	ONGOING
Closed circuit television	MEDIUM	HIGH	HIGH	ONGOING
Alarms/call boxes	MEDIUM	MEDIUM	MEDIUM	ONGOING

FIGURE 2 Assessing physical assault.

- Those solutions should be in terms of the establishment of detailed procedures that are well documented and tested before adoption.
- Develop and implement an initial training and retraining program for all transit personnel regarding the procedures associated with each of the security problems.
- Once everyone is initially trained, institute the procedures.
- This entire process should be dynamic. Nothing stays the same, and new information is gathered on a regular basis. It is important for the system to review and update its procedures regularly.

ACKNOWLEDGMENTS

The Ketron Division of the Bionetics would like to extend its full appreciation to FTA, the Volpe National Transportation Systems Center, and the following individuals who were instrumental in initiating this project and bringing it to a successful completion: Franz Gimmler, Deputy Associate Administrator for Safety, FTA, and Judy Meade, Program Manager, FTA. Complete copies of the *Transit Security Procedures Guide* and the *Transit System Security Programming Guide* are available from the Volpe National Transportation Systems Center and FTA.